S.L 1 5 PAGE 6 7

(3)

No. 90-1876

Supreme Court, U.S.
FILED
AUG 6 1991
OFFICE OF THE CLERK

IN THE

SUPREME COURT OF THE UNITED STATES

OCTOBER TERM, 1990

ROBERT TAPPAN MORRIS,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE
UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

BRIEF FOR THE *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION SUPPORTING PETITIONER

ERIC M. LIEBERMAN
NICHOLAS E. POSER
RABINOWITZ, BOUDIN, STANDARD,
KRINSKY & LIEBERMAN
740 Broadway, 5th Floor
New York, New York 10003
(212) 254-1111

HARVEY A. SILVERGLATE*
THOMAS C. VILES
SILVERGLATE & GOOD
Boston, Massachusetts 02110
(617) 542-6663

*Counsel of Record

MICHAEL GODWIN
ELECTRONIC FRONTIER FOUNDATION
155 Second Street
Cambridge, Massachusetts 02141
(617) 864-0665

Attorneys for the Amicus Curiae

August 6, 1991

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTEREST OF THE AMICUS CURIAE 1

STATEMENT 3

SUMMARY OF THE ARGUMENT 8

ARGUMENT 8

CONCLUSION 17

TABLE OF AUTHORITIES

CASES

Bell v. *United States*,
349 U.S. 81 (1955) 11

Blum v. *Stenson*,
465 U.S. 886 (1984) 9, 10

Chapman v. *United States*, U.S. ,
111 S.Ct. 1919 (1991) 11

Ladner v. *United States*,
358 U.S. 169 (1958) 11

Liparota v. *United States*,
471 U.S. 419 (1985) 10, 12

Morisette v. *United States*,
342 U.S. 246 (1952) 13

Moskal v. *United States*, U.S. ,
111 S.Ct. 461 (1990) 11

New York Times Co. v. *Sullivan*,
376 U.S. 254 (1964) 14

Rewis v. *United States*,
401 U.S. 808 (1971) 11

United States v. *Bass*,
404 U.S. 336 (1971) 10, 11, 12

United States v. *Five Gambling Devices*,
346 U.S. 441 (1953) 11

United States v. *Marvin*,
687 F.2d 1221 (8th Cir. 1982) 13

United States v. *Morris*,
928 F.2d 504 (2d Cir. 1991) 8, 9, 10, 13

United States v. *Nofziger*,
878 F.2d 442 (D.C.Cir. 1989),
cert. denied, U.S. ,
110 S.Ct. 564 (1989) 13

United States v. *United States Gypsum Co.*,
438 U.S. 422 (1978) 11, 12

United States v. *Universal C.I.T. Credit Corp.*
344 U.S. 218 (1952) 11

CONSTITUTION AND STATUTES

U.S. Constitution,
First Amendment 1, 6, 7

18 U.S.C. §1030 Computer Fraud and Abuse Act ("CFAA") . . . . . *passim*

18 U.S.C. §§ 2510 *et seq.* (Title III) 7

18 U.S.C. §§ 2701 *et seq.* (Electronic Communications Privacy Act) 7

42 U.S.C. §§2000aa *et seq.* (First Amendment Privacy Protection Act) 7

N.Y.P.L. §156.05 14

N.Y.P.L. §156.10 14

N.Y.P.L. §156.20 14

N.Y.P.L. §156.25 14

N.Y.P.L. §156.30 14

N.Y.P.L. §156.35 14

OTHER AUTHORITIES

132 Cong.Rec. H3275 (June 3, 1986) 10

132 Cong.Rec. H9260 (Oct. 6, 1986) 10

H.R.Rep. No. 612, 99th Cong., 2d Sess. (1986) 10

S.Rep. No. 432, 99th Cong., 2d Sess. (1986), reprinted in 1986 U.S. Code Cong. & Admin. News 2479 10

American Law Institute, Model Penal Code §2.02(4) (Prop.Off.Draft 1962) 12

J. Barlow, *Crime and Puzzlement* (1990) 5

Becker, *The Liability of Computer Bulletin Board Operators for Defamation Posted by Others*, 22 Conn.L.Rev. 203, 204 (1989) 5

Common Electronic Policy, The Economist, Feb. 16, 1991, at 24 . . . . . 5, 6

Figallo, *Defending the New Frontier*, Index on Censorship, July 1991, at 25 5

Kapor, *Why Defend Hackers?* EFF News, Dec. 10, 1990 (available electronially on the WELL, eff conference) 5

Note, *An Electronic Soapbox: Computer Bulletin Boards and the First Amendment*, 39 Fed.Comm.L.J. 217 (1988) 4

I. de Sola Pool, *Technologies of Freedom* (1983) 6, 16

Silverglate & Viles, *Constitutional, Legal and Ethical Considerations for Dealing with Electronic Files in the Age of Cyberspace*, 1991 Federal Enforcement 239 (Georgetown Univ.) 5

"This LAN is my LAN," or Hard Disks Make Hard Law, 5 BNA Crim.Prac. Manual 264 (May 29, 1991) 5

L. Tribe, *American Constitutional Law* (1988) 6, 16

INTEREST OF THE AMICUS CURIAE

The *amicus curiae* Electronic Frontier Foundation ("EFF") is a privately funded, tax-exempt, nonprofit organization concerned with the legal, technical, and social problems posed by the applications of new computing and telecommunications technology. Its founders include Mitchell Kapor, a leading pioneer in computer software development who founded the Lotus Development Corporation and developed the Lotus 1-2-3 Spreadsheet software, and Steven Wozniak, co-founder of Apple Computers, Inc. As set forth in its founding statement, EFF's organizational goals are the following:

> Engage in and support educational activities which increase popular understanding of the opportunities and challenges posed by development in computing and telecommunications.
>
> Develop among policy-makers a better understanding of the issues underlying free and open telecommunications, and support the creation of legal and structural approaches which will ease the assimilation of these new technologies by society.
>
> Raise public awareness about civil liberties issues arising from the rapid advancement in the area of new computer-based communications media. Support litigation in the public interest to preserve, protect, and extend First Amendment rights within the realm of computing and telecommunications technology.

Encourage and support the development of new tools which will endow non-technical users with full and easy access to computer-based telecommunications.

EFF is barely one year old, and its membership is growing rapidly. EFF's members are mainly professionals involved in computer research and technology, academics and students working in computer-related disciplines, amateur computer enthusiasts, and legal professionals who practice in the areas of constitutional and computer law. EFF's founders and members therefore are uniquely well informed about the capabilities of the new technologies, as well as about issues which concern the national computing community.

EFF is implacably opposed to computer trespass and theft, and it does not condone any unauthorized tampering with computers. Indeed, EFF's unequivocal belief is that the security of private computer systems and networks is both desirable and necessary to the maintenance of a free society. But EFF's founders and supporters also believe that the law's development lags far behind advances in computing and telecommunications technology. They hope that this distance can be closed by informed policy-making and adjudication.

EFF's interest in cases such as this is to promote a legal climate where the electronic communication systems do not become chilly preserves of legal authoritarianism unworthy of the technology's central role in open, democratic society.

In a free society, new laws should express society's will. However, in the process of legislation and the articulation of the decisional law, the cure for one perceived computer law problem

potentially can create a host of unwarranted new burdens on the citizen's freedom to communicate using new computer-related media. The continuing vitality of the new technologies demands that the developing law which regulates computer use jealously guard fundamental freedoms.

The present case demonstrates the gulf which exists between the state of the law and the state of the new technology. It underscores the need for the considered development of a legal framework in which both the security of computer systems can be protected, and the ability of system users to communicate, conduct research, and to exchange ideas will not be fettered. EFF's principal concern is that the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. §1030, as construed by the courts below, conflicts with the precedents of this Court governing statutory construction, and it will substantially hamper the development of new computing and communications technologies.

By the broad gloss which has been given to the statute in this case, the CFAA would impose strict felony liability for harms which computer users caused through sheer inadvertence. The CFAA's construction in the Second Circuit bodes ominously for the future applications of a technology which inevitably will pervade virtually every aspect of civil society.

This brief is filed with the written consent of all parties.

STATEMENT

Robert Tappan Morris's petition raises a question of statutory construction which has important implications for the future of computer use. The outcome of the case will determine

whether unintended conduct can be the basis of a felony criminal conviction under the Computer Fraud and Abuse Act, 18 U.S.C. §1030. This case may determine whether millions of citizens who use computers shall do so at their own peril, or free from fear of unpredictable criminal sanctions.

Originally created for business uses, the new computing and telecommunications technologies are rapidly changing the face of civil society. Personal computers (and the people who operate them) are becoming more closely linked to each other in various small networks. These networks, in turn, are becoming joined together in larger, global networks. The practical consequence of this linkage is that every person who has access to a small personal computer and a telephone line can communicate instantaneously with every other person in the world so equipped. *E.g.*, Note, *An Electronic Soapbox: Computer Bulletin Boards and the First Amendment*, 39 Fed.Comm.L.J. 217, 218-21 (1988). These technologies are providing new media for the dissemination of information, and new forums for the free exchange of views. Academic institutions and scholars, natural scientists, members of every profession, political activists, archaeologists, amateur hobbyists, journalists and news services, literary critics, musicologists, and every other conceivable grouping of people in society now can communicate with each other simultaneously on topics of common interest.

The three most popular forms of network communications are electronic mail ("e-mail"), online publications, and electronic conferencing systems (or, "bulletin boards"). *See generally* Note, *An Electronic Soapbox*, *supra*, at 218-21. E-mail, like its postal ancestor, enables computer users to send individual messages to each other in private. Unlike surface mail, however, such

communication can take place in a matter of seconds. Online publications are similar to printed periodicals, but they are delivered to subscribers through various telecommunication networks. Electronic bulletin boards provide a forum for numerous participants to discuss topics simultaneously. The electronic publications and bulletin boards currently provide forums for the discussion of a multiplicity of topics, "from apiarists to Zoroastrians," and have been appropriately compared to the electronic version of Main Street or a town meeting. J. Barlow, *Crime and Puzzlement*, 2-3 (1990); *see also "This LAN Is My LAN," or Hard Disks Make Hard Law*, 5 BNA Crim.Prac. Manual 264 (May 29, 1991); Kapor, *Why Defend Hackers?*, EFF News, Dec. 10, 1990 (available electronically on the WELL, eff conference); Becker, *The Liability of Computer Bulletin Board Operators for Defamation Posted by Others*, 22 Conn.L.Rev. 203, 204 (1989) (electronic bulletin board described as "a kind of computerized Democracy Wall -- on which users can post whatever information they desire, and from which users can retrieve information provided by others"); *see generally*, Figallo, *Defending the New Frontier*, Index on Censorship, July 1991, at 25.

Recently, in the academic computer conferences alone, the volume of message traffic has been increasing at *monthly* rates of between thirty and forty percent. *Common Electronic Policy*, The Economist, Feb. 16, 1991, at 24. Each of the two largest computer networks in the United States, Internet and CompuServe, are estimated to have more than 500,000 subscribers, and each in turn is composed of some 2,000 smaller computer networks. *Id.*

Recently, attention has been given to proposals to develop a new National Research and Education Network ("NREN"), capable of handling high volumes of computer traffic at rates many times

faster than current networks. *See, e.g.*, Silverglate & Viles, *Constitutional, Legal, and Ethical Considerations for Dealing with Electronic Files in the Age of Cyberspace*, 1991 Federal Enforcement 239, 243 (Georgetown Univ.); *Common Electronic Policy*, *supra*, at 24. Such networks will enable the interconnection of virtually everyone in the United States.

Accordingly, the computing and telecommunication technologies which have occasioned the present case must be more broadly viewed. They promise to give society convenient and inexpensive means of communication and association in the near future, and they form the basis for the primary communications media and forums of the next century.

The new technologies also are likely to challenge many traditional notions of the proper place of the press and electronic media in the constitutional scheme. Computing technologies soon will rival books, newspapers, television, radio and the mails as means by which people communicate. Ultimately, the new technologies very likely will supplant other known forms of communication, and may demand the substantial extension and revision of the judicial doctrines which have been articulated under the First Amendment. As commentators point out, communications in our society are becoming less dependent on paper; writings need not be *printed* in order to convey ideas. *E.g.*, I. de Sola Pool, *Technologies of Freedom* 41-42 (1983). In Professor Laurence Tribe's words, "As computer terminals become ubiquitous and electronic publications expand, the once obvious boundaries between newspapers and television, telephones and printing presses, become blurred." L. Tribe, *American Constitutional Law* § 12-25, at 1009 (1988).

It is important to note that these new communications technologies, in their earliest infancy, are becoming the subject of precedent-setting litigation, before their fullest capabilities can be known or appreciated. As described herein, legal precedents established now can radically affect the course of the computer technology's future, and with it the fate of an important tool for the exchange of ideas in a democratic society. Where the law limits or inhibits the use of these new technologies, concerns of constitutional dimension inevitably arise. In cases such as the present one, close attention should be given to the potential reverberations on activities protected by the First Amendment.[1]

---

[1] It is significant that the Electronic Communications Privacy Act ("ECPA") was enacted five days after the enactment of the CFAA provision now under consideration. Pub.L. 99-508, Title II, § 201, 100 Stat. 1860-68 (Oct. 21, 1986), *codified at* 18 U.S.C. §§ 2701 *et seq.* The ECPA closely regulates the circumstances in which a computer conference operator can reveal a third-party subscriber's e-mail messages, and the conditions under which a government agency can subpoena such material. *See* 18 U.S.C. §§ 2703-2705. It also creates civil remedies for the subscriber whose electronic messages have been disclosed without authorization. 18 U.S.C. § 2707.

By this contemporaneous enactment, Congress reiterated its longstanding policy to give heightened protection to civilian electronic communications. *Compare* 18 U.S.C. §§ 2510 *et seq.* ("Title III," enacted in 1968, which strictly controls the interception of wire and electronic communications); 42 U.S.C. §§ 2000aa *et seq.* (First Amendment Privacy Protection Act, enacted in 1980, which limits searches and seizures of materials, including "electronically recorded cards, tapes, or discs," intended for dissemination through the news media, including "broadcast, or other similar form of public communication").

SUMMARY OF THE ARGUMENT

This case is the first in which the courts have given full appellate consideration to the construction of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. The Court of Appeals below interpreted the CFAA to criminalize conduct regardless of the defendant's mental state. That holding conflicts with decisional law of this Court guiding the interpretation of criminal statutes. If allowed to stand, the decision of the Court of Appeals well may transform otherwise law-abiding computer users into felons, and inhibit the creative uses of computer technology.

ARGUMENT

The parties never seriously disputed the relevant facts of this case. The United States contended that the petitioner, Robert Tappan Morris, intentionally accessed various computers on the Internet computer network with a program of his own design, called a "worm". *E.g.*, *United States* v. *Morris*, 928 F.2d 504, 505 (2d Cir. 1991); Brief for the United States, *United States* v. *Morris*, No. 90-1336 (2d Cir., filed Oct. 19, 1990)("Gov't 2d Cir. Brief") at 2-12. The petitioner agrees with that assertion. *E.g.*, Petition, at 4-5. The United States has argued that petitioner gained this access without authority. *E.g.*, Gov't 2d Cir. Brief at 36-48. The petitioner does not challenge that point here. Petition at 7 n. 4. Both sides agree that through sheer inadvertence, Morris caused many computer systems on the Internet to slow down or temporarily cease to function. *E.g.*, Petition at 5-6; Gov't 2d Cir. Brief at 12-16. Significantly, both sides also agree that Morris did not intend to harm any computer with his "worm", nor did he intend or expect to prevent anyone else from using any computer. *E.g.*, Petition at 4; Gov't 2d Cir. Brief at 6 (citing evidence that

petitioner designed his program to "do absolutely nothing" except enter computers). Instead, "[t]he worm was supposed ... not to interfere with normal use of the computers" on the Internet. *United States* v. *Morris*, *supra*, 928 F.2d at 505. Indeed, the facts point to the opposite conclusion -- that Morris's conduct was calculated *not* to damage any computers or prevent their use -- and the United States does not dispute this. The subsequent injuries to various computers were completely accidental. *Id.* at 506.

The case boils down to the critical question of whether Morris violated §1030(a)(5) of the CFAA,[2] notwithstanding his obvious efforts to do no harm. Specifically, can petitioner be guilty of having violated the CFAA, in the absence of any proof or claim that he intended the proscribed injury?

The law of this case is that the meaning of § 1030(a)(5) cannot be deduced from its plain language. *See United States* v. *Morris*, 928 F.2d 504, 507 (2d Cir. 1991).[3] It is well established that, when the meaning of a statute is unclear on its face, the court

---

[2] In pertinent part, 18 U.S.C. § 1030(a)(5) makes it a crime to "intentionally access a federal interest computer without authorization, and by means of such conduct ... prevent[] authorized use of any such computer or information," when such conduct inflicts injuries costing at least $1000. In this case, the term "federal interest computer" simply means that all of the computers involved were not located in the same State. *See* 18 U.S.C. § 1030(e)(2). The parties also did not dispute that jurisdictional fact.

[3] Moreover, the record amply illustrates that, as a practical matter, different courts reading the statute can arrive at opposite conclusions about whether the statute's meaning is plain. On the one hand, the District Court for the Northern District of New York concluded that the language of the statute *was* clear on its face, *see* Transcript of Decision *United States* v. *Morris*, No. 89-CR-139 (N.D.N.Y., Nov. 3, 1989), reprinted in Appendix B to Petition, at 48a-49a. On the other hand, the Court of Appeals for the Second Circuit found that it *was not* clear. *See United States* v. *Morris*, *supra*, 928 F.2d at 507.

should look to the intent of the legislature which enacted it. *E.g.*, *Liparota* v. *United States*, 471 U.S. 419, 424-25 (1985); *Blum* v. *Stenson*, 465 U.S. 886, 896 (1984); *United States v. Bass*, 404 U.S. 336, 341-42 (1971). Here, in support of their contentions, both sides referred to Congressional activity at significant junctures in the CFAA's legislative history. EFF agrees with the petitioner's interpretation of the legislative history, for the weight of the record of § 1030(a)(5)'s enactment shows Congress's purpose to criminalize intentional injuries, as opposed to all injuries.[4] However, even if the Court were to find persuasive those other parts of the legislative history, which suggest a contrary result,

---

[4] For example, the petitioner can point to the Senate Judiciary Committee's consideration of §1030(a)(5); the Committee Report stated that the word "intentionally" requires that "the causing of the result must have been the person's conscious objective." S.Rep. No. 432, 99th Cong., 2d Sess. 10 (1986), *reprinted in* 1986 U.S. Code Cong. & Admin. News 2479, 2484. Elsewhere, the Report reiterates that §1030(a)(5) is "designed to penalize those who intentionally alter, damage, or destroy certain computerized data belonging to another." S.Rep. No. 432, *supra*, at 10, 1986 U.S. Code Cong. & Admin. News at 2488. Furthermore, the House Judiciary Committee report characterized §1030(a)(5) as a "'malicious damage' felony violation." H.R.Rep. No. 612, 99th Cong., 2d Sess., at 7 (1986). According to the House Committee, the purpose of the provision was to deter conduct which is "intended to alter another's computer password," and the like. H.R.Rep. No. 612, *supra*, at 12. *See also* 132 Cong.Rec. H3275, H3276 (June 3, 1986) (remarks of Rep. Hughes: section 1030(a)(5) creates "a 'malicious damage' felony" offense); *id.* at H3278 (remarks of Rep. Rodino: section 1030(a)(5) proscribes "malicious damage" of more than $1,000); 132 Cong.Rec. H9260, H9262 (Oct. 6, 1986) (Rep. Hughes describes offense under §1030(a)(5) as "a malicious damage felony violation").

There is far less in the record of § 1030(a)(5)'s enactment which the government can marshal to use. However, in the courts below the government principally relied on arguments which concentrated on § 1030(a)(5)'s textual differences from other subsections of the Act, and on some of its stylistic differences from the provisions of an earlier version of the CFAA. *See* 18 U.S.C. § 1030 (Supp. II, 1984); *United States* v. *Morris*, *supra*, 928 F.2d at 508-09.

then the record of §1030(a)(5)'s enactment is equivocal, and another guide to statutory construction must be used.

It is a well-established rule of criminal statutory construction that, where both the plain language and the legislative history do not avail, the courts should apply the rule of lenity to problems of the construction and interpretation of criminal statutes. *E.g.*, *Rewis* v. *United States*, 401 U.S. 808, 812 (1971); *Bass*, *supra*, 404 U.S. at 347 (*citing Ladner* v. *United States*, 358 U.S. 169, 177 (1958); *Bell* v. *United States*, 349 U.S. 81 (1955); *United States* v. *Five Gambling Devices*, 346 U.S. 441 (1953)). As this Court has directed,

> when choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite.

United States v. *Universal C.I.T. Credit Corp.*, 344 U.S. 218, 221-22 (1952) (Frankfurter, J.). *See also Chapman* v. *United States*, U.S. , 111 S.Ct. 1919, 1926-27 (1991); *Moskal* v. *United States*, U.S. , 111 S.Ct. 461, 465 (1990); *United States* v. *United States Gypsum Co.*, 438 U.S. 422, 437 (1978).

Applying the rule of lenity to the present case, the CFAA must be read to impose a *mens rea* requirement on the element which describes the injury. Here, the rule directs that, absent a showing that Morris intended to do the harm which the CFAA proscribes -- in other words, evidence that he intended to prevent another from using a federal interest computer -- the petitioner cannot be convicted of a violation of the CFAA.

Application of the rule of lenity here is consistent with the petitioner's right to be on notice of the requirements of the law and charges against him. Here, the rule would best afford otherwise law-abiding computer users adequate notice of the sort of conduct which is unlawful, and give them the opportunity to avoid violating the law unknowingly. *See, e.g., Liparota, supra,* 471 U.S. at 427.

By requiring the resulting harm to be intentional, the application of the rule of lenity here would comport with other authoritative guides to statutory interpretation. Under the Model Penal Code, for example, a culpable mental state must be proven for each element of a serious crime:

> When a law defining an offense prescribes the kind of culpability that is sufficient for commission of the offense without distinguishing among the material elements thereof, such provision shall apply to all the material elements of the offense, unless a contrary purpose plainly appears.

American Law Institute, Model Penal Code §2.02(4) (Prof.Off.Draft 1962); *see also United States Gypsum Co., supra,* 438 U.S. at 436-37. Additionally, as a general rule an ambiguity in a criminal statute should be resolved in favor of the narrower of two possible readings. *Bass, supra,* 404 U.S. at 348. Finally, such a result would be consistent with the disfavored status accorded to criminal offenses requiring no *mens rea. See, e.g., Liparota, supra, 471 U.S. at 426; United States Gypsum Co., supra,* 438 U.S. at 438. This is especially so in a case like the present one, where the statute in question criminalizes a broad range of conduct. *Liparota, supra,* 471 U.S. at 426.

Thus, regardless of whether the legislative history is clear or not, the Court of Appeals for the Second Circuit erred when it found that Congress intended no *mens rea* requirement to be imposed on the injury element of the felony defined by § 1030(a)(5). *See United States* v. *Morris*, *supra*, 928 F.2d at 508-09.

It is one matter to hold the reckless mischief-maker, or even the negligent tinkerer, civilly liable for unintentionally caused inconvenience and harm. But it is entirely contrary to our notions of justice to brand as a felon the computer user who did not intend to do harm -- especially a computer user like Morris who had taken pains to avoid doing any injury at all. The notion that a culpable mind is a necessary component of criminal guilt is "as universal and persistent in mature systems of law as belief in freedom of the human will and a consequent ability and duty of the normal individual to choose between good and evil." *Morisette* v. *United States*, 342 U.S. 246, 250-51 (1952)(Jackson, J.). As one court recently observed, "[u]sually the stigma of criminal conviction is not visited upon citizens who are not morally to blame because they did not know they were doing something wrong." *United States* v. *Nofziger*, 878 F.2d 442, 452-53 (D.C.Cir. 1989) (Buckley, J., quoting *United States* v. *Marvin*, 687 F.2d 1221, 1226 (8th Cir. 1982)), *cert. denied*, U.S. , 110 S.Ct. 564 (1989).

The United States has contended for a reading of the CFAA which would require that the defendant had intended only to "access" a computer without authority; the subsequent harms done need not have been intended in order to result in a conviction under the Act. Such a construction not only ignores the applicable rules of statutory construction; it also defies common sense. According to the United States' view, a defendant's inadvertent entry into a

computer would absolve the defendant of any subsequent malicious conduct; *no* criminal liability would attach to the accidental intruder who, upon realizing the error, proceeds to *intentionally* and maliciously damage a computer.[5]

It would send a chilling message to computer users -- including people whose livelihoods depend on computers, and those who have dedicated their lives to the advancement of computing sciences -- to allow the decision of the Court of Appeals below to stand. The Constitution clearly disfavors laws which attach liability without fault for communicative conduct, for the very existence of such laws, whether enforced or not, can abolish critical portions of the public discourse. *See, e.g., New York Times Co.* v. *Sullivan*, 376 U.S. 254, 271-79 (1964). Should it remain the adjudicated law that, under the CFAA, strict criminal

---

[5] Petitioner would fare far worse under the harsh reading of the CFAA that the United States and the Court of Appeals has adopted than he would under applicable New York computer crime statutes.

For example, in New York, Unauthorized Use of a Computer is a misdemeanor which prohibits the "knowing" use of the computer of another without authority. N.Y.P.L. § 156.05. A separate misdemeanor, Second Degree Computer Tampering, proscribes the "intentional[]" alteration or destruction of computer data. N.Y.P.L. § 156.20. The relevant New York computer *felonies* require proof of a *mens rea* element with respect to the results of defendant's conduct. *See, e.g.*, N.Y.P.L. § 156.25 (First Degree Computer Tampering consists of the elements of Second Degree Computer Tampering *plus* "intent" or "attempt" to commit a felony, or "intentional[]" altering or destroying of computer data); N.Y.P.L. § 156.10 (Computer Trespass consists of "knowing[]" use of a computer without authorization plus "knowing[]" access to private computer data, or an "intent" or "attempt" to commit a felony); N.Y.P.L. § 156.30 (Unlawful Duplication occurs when computer data are duplicated *and* the owner thereof is thereby "intentionally and wrongfully" deprived of value worth $2500, or duplication done with "intent" or "attempt" to commit felony); N.Y.P.L. § 156.35 (Criminal Possession occurs when defendant "knowingly" possesses computer data or programs without right to do so, *and* defendant has "intent" to benefit someone other than true owner).

liability can be imposed even where absolutely no harm was intended -- and even where the defendant has taken every conceivable measure to avoid any injury -- then computer researchers will infer that scientific inquiry and technological advancement well could mean automatic and unavoidable felony charges. The effects on future exploration into the useful applications of the new technologies -- including, significantly, research in the field of computer security -- will be felt immediately. Since error is an integral part of fruitful computer research, inquiry will be deterred, and advancement in this technological field (one of the remaining few in which this Nation still holds a position of primacy) will be slowed.

Finally, in view of the fact that the new communications technologies at issue here are developing into popular media for scientific, social, political, and artistic discourse, EFF respectfully urges the Court to closely examine laws, like the one presently at issue, which can be used to impose strict felony liability for communicative and expressive conduct. An interpretation of the CFAA which is so draconian as to burden and distort the development of popular communications cries out for close scrutiny. As Professor Tribe observed,

> The rate of technological change has outstripped the ability of the law, lurching from one precedent to another, to address new realities. Novel communications are pressed into service while still in their infancy, and the legal system's initial encounters with these newborns have a lasting influence. . . "[t]echnical laymen, such as judges, perceived the new technology in that early, clumsy form, which then becomes their image of its nature, possibilities,

> and use. This perception is an incubus on later understanding."

L. Tribe, *American Constitutional Law* § 12-25, at 1007 (1988) *quoting* I. de Sola Pool, *Technologies of Freedom*, *supra*, at 7.

Accordingly, the Electronic Frontier Foundation as *amicus curiae* supports the Petition for Certiorari now before the Court. In the interests of fostering the development of new technologies, and securing an electronic environment which promotes the free exchange of ideas as well as privacy, EFF asks this Court to review the question of statutory interpretation which this controversy raises.

CONCLUSION

For the foregoing reasons, the *amicus curiae* Electronic Frontier Foundation urges the Court to grant the Petition of Robert Tappan Morris for a Writ of Certiorari to the United States Court of Appeals for the Second Circuit.

August 6, 1991

Respectfully submitted,

HARVEY A. SILVERGLATE*
THOMAS C. VILES
SILVERGLATE & GOOD
89 Broad Street, 14th Floor
Boston, Massachusetts 02110
(617) 542-6663
**Counsel of Record*

ERIC M. LIEBERMAN
NICHOLAS E. POSER
RABINOWITZ, BOUDIN,
STANDARD, KRINSKY,
& LIEBERMAN, P.C.
740 Broadway, 5th Floor
New York, New York 10003
(212) 254-1111

Attorneys for the *Amicus Curiae*